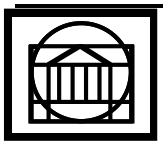
SAFETY CASE

Authors	Approved	Date
Ted Giras, Ph.D., Principal Investigator		
Lori M. Kaufman, Ph.D.		



School of
Engineering and Applied Science
Center for Safety-Critical Systems
University of Virginia

MTA New York City Transit

Abstract

The Railroad Safety Advisory Committee (RSAC) Processor-based Regulatory Rule establishes the “safety case” fundamentals. These fundamentals present a precise and rigorous proof-of-safety argument using “clear and convincing evidence” that the replacement system increases the safety as compared to the existing. The supplier prepares the safety case for review by a third party independent assessor, and the findings are submitted to the Federal Railroad Administration (FRA). The FRA reviews the safety case, and if it deemed sufficient, then approval to proceed with the replacement system deployment is granted.

Table of Contents

Glossary

component: a subset of a subsystem that provides a specified functionality as part of the total subsystem functionality.

hazard: an existing or potential event creating a condition that perturbs normal operation of a system, sub-system or component that if goes undetected may lead to an unsafe failure.

mean time to hazardous event: the expected time to the occurrence of a hazardous event in a subsystem or a component.

subsystem: a subset, SS, of a system that provides a specified functionality as part of the total system functionality.

system: a collection of subsystems and/or components that when interconnec ted provide a specified functionality; that is, System Functionality = f(SS, C, R), where SS and C are the subsystem and component sets and R is the set of relationships that interconnect the subsystem and component interfaces that combine them into a coherent whole.

Acronyms

FRA: Federal Railroad Authority

MTTHE: Mean Time ToHazardous Event

PSP: Product Safety Plan

RSAC: Railroad Safety Advisory Committee

RSPP: Railroad Safety Program Plan

TMA: Traffic Management Algorithm

1 Introduction

Prior to deploying any new product, the railroad and supplier communities must demonstrate that the new product's safety. In order to demonstrate such safety using the Railroad Safety Advisory Committee (RSAC) processor-based regulatory rule, two safety plans are required: (1) a Railroad Safety Program Plan (RSPP) and (2) a Product Safety Plan (PSP). Each Railroad must prepare a RSPP as a formal document. This document describes a railroad's strategic process for addressing the Railroads safety hazards and their mitigation using application-specific safety products, which can be either a system, subsystem or component. The RSPP specifies the process(es) to be executed to ensure application-specific safety for the product. The RSPP strategy is implemented though the use of PSP that must be prepared for each application-specific product as described in § 236.905 RSAC Processor-based Regulatory Rule.

The Railroad and the Supplier develop a Product Safety Plan (PSP) for each application-specific safety product to be deployed by the railroad. Each PSP must be approved by the FRA prior to any deployment of the specified product. The PSP must provide complete documentation supporting § 236.907 of the RSAC Processor-based Regulatory Rule. From this rule, the PSP must describe in detail all of the safety aspects of the product including procedures for its development installation, implementation, operation, maintenance, repair, inspection, testing and modification, as well as analyses supporting its safety claims.

Using the process defined by the RSPP and the safety claims developed by the PSP, a safety case is constructed using formal arguments to demonstrate with "clear and convincing evidence" that the new product increases safety relative to the existing product. The Safety Case argument is supported with both qualitative and quantitivate safety behavioral evidences that are derived from rigorous analyses of the data provided by the PSP. Once the safety case is completed, then a third party independent assessor audits the findings. Once this audit is complete, including any needed revisions, then the safety case is submitted to the Federal Railroad Authority (FRA). If after FRA review it is determined that the safety case sufficiently analyzes the product, then the FRA grants

the requesting railroad permission to deploy the new product. Thus, the construction of the safety case is a critical path in the deployment of new products. Therefore, it is imperative that great care must be taken in developing a safety case.

2 Safety Case Taxonomy

The safety case consists of both qualitative and quantitative analyses. These analyses use the information provided in the PSP to validate and to verify the safety claims presented. An important aspect of the of the safety case taxonomy is the completeness of the PSP. As a minimum, the PSP must provide the following qualitative and quantitative elements to support the construction of a quantified proof-of-safety:

- Description of Product
- Description of Railroad Operation
- Operational Concepts Documentation
- Safety Requirements Document
- Product Architecture
- Hazard Log
- Risk Assessment
- Hazard Mitigation Analysis
- Description of Safety Assessment Validation &Verification Processes
- Safety Assurance Concepts
- Human Factors Analysis
- Training Requirements
- Test Procedures and Equipment
- Part 236 Rules and Regulations
- Security Measures for the Product
- Warnings and Warning Labels
- Implementation Testing Procedures
- Records Necessary to Ensure Product Safety (Customer Generated)
- Safety-critical Assumptions & Backup Methods of Operation
- Incremental & Predefined Changes (Note – None may be planned)

Once the PSPS has been reviewed and it has been determined that it includes all pertinent qualitative and quantitative safety information, then the formulation of the safety case can commence. The safety case is partitioned into two distinct portions. Part I consists of the qualitative validation of the PSP, which includes a rigorous review of the PSP completeness. Part II provides the quantified verification of the information presented in the PSP and its associated safety claims. Ata minimum, the complete safety case must address and include the following:

- DEFINITIONS: All the definitions associated with the safety claims and the constructs of the proof-of-safety shall be defined.
- BASIC SAFETY PRINCIPLES: The basic safety-critical principles that support the safety claims shall be documented and reviewed for completeness.
- ASSUMPTIONS: The assumptions related to the basic safety principles, potential failure modes and safety claims shall be categorized and reviewed for applicability and completeness.
- TRACK PLAN APPLICATION-SPECIFIC INFRASTRUCTURE: The risk assessment shall be demonstrated for a specific train line. It shall include the track plan infrastructure, which can include track segments, curves, bridges, highway grade crossings, switches, signals, track circuits and any related wayside and track devices that impact safety.
- THROUGHPUT CAPACITY SCHEDULING: A traffic management algorithm (TMA) that schedules train movement shall be included to ensure the estimation of risk exposure. The TMA shall be used to determine the risk for a given train that is coincident in time and position with a given hazard.
- TRAIN MOVEMENT RULES: The train movement rules that determine the operational behavior of the system and regulate the movement of trains in presence of hazards shall be included. These rules shall be evaluated on a train-centric basis and are train system specific.
- HUMAN-BEHAVIOR ANAYSIS: The bavior of the dispatcher, train crews and roadway workers shall be included in the risk assessment by modeling their effect on the train movement rules.

- HAZARDS IDENTIFICATION, ANALYSIS AND MITIGATION: A detailed list of the hazards to be mitigated by the signaling and train control system shall be included and their effect on the train-centric system shall be incorporated in the risk assessment.
- PROBABILISTIC PROOF-OF-CORRECTNESS (VALIDATION): Risk assessment experiments shall be conducted to demonstrate that the design of the system to be deployed is correct in the hazard-free environment; that is, all the safety-critical devices shall have coverage of 100% and operate without failure.
- PROBABILISTIC PROOF-OF-INCREASE IN SAFETY (VERIFICATION): Risk assessment experiments shall be conducted to demonstrate that the system to be deployed operates correctly in the non hazard-free environment
- PROBABILISTIC PROOF-OF-MTTHE COMPLIANCE: A proof-of-MTTHE compliance, as allocated by the risk assessment, shall be constructed for all of the devices considered by the system risk assessment. The MTTHE proof shall be based on the development of analytical model(s) whose parameters are verified with experimentation on the actual integrated hardware/software system.

2.1 Part 1: Safety Case Qualitative Validation

In Part I, the safety case must review and evaluate all of the PSP documentation. This qualitative analysis must reflect the overall completeness of the information presented in the PSP. This qualitative validation shall provide the third party independent assessor with “creditable and convincing evidences” that ***validates*** the safety compliance of the PSP and its compliance to the RSPP.

2.2 Part II: Safety Case Quantified Verification

Part II of the safety case develops the quantified verification of the PSP for reviewed by the third party independent assessor. This quantified verification shall be structured as a rigorous and formal proof-of-safety argument. Its basis is the probabilistic risk assessment of the effects of a new system deployment on the train line. As part of the quantified proof-of-safety, the MTTHE compliance of all the safety-critical subsystems

and component devices contained in the system as allocated by the risk assessment must be verified. This verification shall demonstrate with “clear and convincing quantified evidences” that the system to be deployed shall provide a significant increase in safety as compared to the existing system to be replaced; that is, this quantification of safety must demonstrate that the

$$Risk_{System\ Deployed} << Risk_{System\ being\ \mathrm{Re}\ placed}$$

subject to “a high degree of confidence and availability” and that “all the devices satisfy the allocated MTTHE compliance.”